

REMARKS

At the time of the Office Action dated October 6, 2004, claims 1-40 were pending. In this Amendment, claims 1, 8, 10, 13-19, 22, 24, 25, 31, 32 and 38-40 have been amended, claims 9, 11, 12, 20, 21 and 23 canceled, and claims 41-43 added. Care has been exercised to avoid the introduction of new matter. Specifically, claims 13 and 22 have been amended to be in independent form. Adequate descriptive support for the amendment of claims 13 and 22 can be found on, for example, page 30, line 6 to page 35, line 17 of the specification (the second embodiment). Claims 31, 38 and 40 have been amended based on claim 24. Adequate descriptive support for new claim 41 can be found on, for example, page 29, line 25 to page 30, line 5 of the specification. Further, new claims 42 and 43 has been added based on, for example, page 39, line 25 to page 42, line 6 of the specification.

Priority is not acknowledged.

Applicants note that the claim for foreign priority and receipt of the certified copies of the priority document filed April 5, 2001, have not been acknowledged. Applicants hereby respectfully request that the Examiner clarify the record by acknowledging the claim for foreign priority and receipt of the certified copies of the priority documents.

Claims 1-40 have been rejected under 35 U.S.C. §102(e) as being anticipated by Boden et al.

In the statement of the rejection, the Examiner asserted that Boden et al. discloses a system and method for managing security objects identically corresponding to what is claimed.

The factual determination of lack of novelty under 35 U.S.C. §102 requires the identical disclosure in a single reference of each element of the claimed invention, such that the identically claimed invention is placed into the possession of one having ordinary skill in the art. *Helifix Ltd. v. Blok-Lok, Ltd.*, 208 F. 3d 1339, 54 USPQ2d 1299 (Fed. Cir. 2000); *Electro Medical Systems S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 32 USPQ2d 1017 (Fed. Cir. 1994).

Based on the above legal tenet, Applicants submit that Boden et al. does not disclose a security communication apparatus, a security communication system, a security communication method and a security information apparatus, including all the limitations recited in claims 1-8, 10, 13-19, 22 and 24-40, as amended.

Specifically, the Examiner asserted that Boden et al. in column 3, line 60 to column 4, line 4; and Fig. 1 anticipates claims 1, 8, 10 and 24. The following is reproduction of the Examiner's cited portion:

Referring to FIG. 1, a Virtual Private Network Connection Model (VPNCM) 14, 15 exists as a database, or other persistent storage medium, on each node 18, 19 in the VPN and executes under control of IKE (an ISAKMP application) and/or some other connection manager application 16, 17 and IPsec 202, 203 on each of initiator node 18 and responder node 19, respectively. These nodes 18, 19 may be host or gateway nodes, or systems, and are referred to as connection endpoints. Once a connection is created, filter rules (or SPD entries) and Security Associations (SAs) are loaded into the IP stack in the kernel 200, 201 to protect the connection's traffic as it passes through the stack.

In response, Applicants submit that it is apparent that the above paragraph is silent on what is claimed in those claims.

Claim 1 recites as follows:

storage means storing associating information that associates user information which can associate a user using the communication terminal on the sending end with a security type that should be applied to the communication of the user; and security type selecting means selecting the security type from the associating information according to the user information, which can specify the user, sent from the communication terminal on a sending end.

Claim 8 recites as follows:

user authentication means authenticating a user using the communication terminal on the sending end; storage means storing associating information which can associate a user using the communication terminal on the sending end with a security type that should be applied to the communication of the user; and security type selecting means selecting the security type from the associating information according to user information which can specify the user authenticated by the user authentication means.

Claim 10 recites “selecting the security type that should be applied to the communication of a user according to information which can specify the user using one of the communication terminals.”

Claims 24 recite that “the security information apparatus provided on the network independently of the first and second communication terminals.” Claims 31, 38 and 40 have been amended to include that limitation recited in claim 24.

Applicants stress that it is apparent that Boden et al., including the Examiner’s cited portion (reproduced above) does not disclose all the limitations recited in claims 1, 8, 10 and 24, as well as claims 31, 38 and 40. Therefore, the reference does not disclose the following advantages provided by the claimed invention:

[S]ince the SPD is configured in advance per user and the SA indicating the contents of the security communication is determined based on the information of the user authentication, it is possible to determine the level of the security communication suitable to that of the user without spoiling the conventional facilities. Page 28, lines 7-11 of the specification.

[S]ince the system is provided with a security information apparatus, a user can determine the proper SA without considering the level of the security communication of the destination. In addition, for instance if the third party manages the security information apparatus, it is possible to optimize the level of the security communication per the service contents provided by the destination, or per the address of the destination. Moreover, the security information apparatus can manage the recommendable SA in centralized by automatically inquiring the corresponding communication terminal of the candidate SA and then collecting the contents, thereby each communication terminal having the IPSEC function can obtain

candidates of the recommendable SA only by inquiring the security information apparatus. Particularly in case of the large-scale network utilizing the IPSEC communication like that a plural company is connected with each other via router including IPSEC function, this system is easy for a user to configure the communication terminal for the security communication, therefore it is effective to reduce the administrator's or user's responsibility. Page 42, lines 7-24 of the specification.

Again, it is submitted that Boden et al. does not have identical disclose of the claimed invention.

With respect to claims 13 and 22, the Examiner asserted that Boden et al. in column 11, line 4-10; and table 1 discloses that "the security type is selected by visually associating the visualized Internet address information with the visualized list of security type."

In response, Applicants emphasize that Boden et al. does not disclose the following limitations recited in claims 13 and 22, as amended:

parameter input window means displaying at least one security type in a way where a security level of the security type is recognizable, and accepting association of a visualized Internet address information with the security type, and

security type selecting means selecting a security type applied to the communication with the communication terminal on the receiving end corresponding to the visualized Internet address information based on the association.

Accordingly, the reference does not disclose the following benefit provided by the claimed invention: "Since the SA can be registered according to the address information specified by the application that is used in general, even a user without a special knowledge can specify the SA easily" (page 35, lines 3-5 of the specification). Moreover, the reference does not disclose the following benefit obtained based on the limitation of "displaying at least one security type in a way where a security level of the security type is recognizable": "The parameter input window [] can display 'high security', 'middle security', 'low security' and 'No security', for example, instead of

displaying a plurality of SA, thereby it comes to be easy for a user to understand the associating of the address information with the SA” (page 35, lines 6-9 of the specification).

Based on the foregoing, Applicants submit that Boden et al. does not disclose all the limitations recited in independent claims 1, 8, 10, 13, 22, 24, 31, 38 and 40, as amended, and therefore, does not have identical disclosure of each element of the claimed invention in the meaning of 35 U.S.C. §102.

It is also noted that a dependent claim is not anticipated if the independent claim upon which it depends is allowable because all the limitations of the independent claim are contained in the dependent claim. Therefore, claims 2-7, 14-19, 25-30, 32-37 and 39 are patentable because they respectively include all the limitations of independent claims 1, 13, 24, 31 and 38. The Examiner’s additional comments with respect to those claims do not cure the argued fundamental deficiencies of Boden et al.

It is further noted that the rejection of claims 9, 11, 12, 20, 21 and 23 has been rendered moot by cancellation of those claims.

Applicants, therefore, respectfully solicit withdrawal of the rejection of the claims under 35 U.S.C. §102(e) and favorable consideration thereof.

New Claims 41-43.

As discussed above, Applicants submit that new claims 41-43 are patentable since they respectively include all the limitations of independent claims 8 and 24.

In addition, Applicants specifically stress that Boden et al. does not disclose a benefit obtained based on claims 42 and 43 as follows:

[T]he security information apparatus can manage the recommendable SA in centralized by automatically inquiring the corresponding communication terminal of

the candidate SA and then collecting the contents, thereby each communication terminal having the IPSEC function can obtain candidates of the recommendable SA only by inquiring the security information apparatus. Particularly in case of the large-scale network utilizing the IPSEC communication like that a plural company is connected with each other via router including IPSEC function, this system is easy for a user to configure the communication terminal for the security communication, therefore it is effective to reduce the administrator's or user's responsibility. Page 42, lines 13-24 of the specification.

Applicants, therefore, respectfully solicit favorable consideration of new claims 41-43.

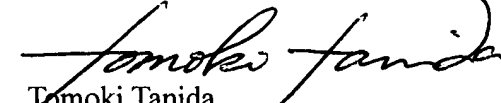
Conclusion.

Accordingly, it is urged that the application is in condition for allowance, an indication of which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, Examiner is requested to call Applicants' attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP


Tomoki Tanida
Recognition under 37 C.F.R. 10.9(b)

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 SAB:TT
Facsimile: 202.756.8087
Date: January 6, 2005

**Please recognize our Customer No. 20277
as our correspondence address.**